How to avoid getting caught Phishing
or
How to avoid giving money to strangers
or
Information Security is everyone's job

Michael Hughes

Principal Consultant

Convergent Informatics Inc.

July 21, 2008

Phishing = con artist

- Phishing is an attempt to criminally and fraudulently acquire sensitive information, such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication
  - PayPal, eBay and online banks are common targets
- Phishing can be done using email, phone, texting, Instant Messaging or even snail mail
- Phishing is an example of *social engineering* techniques used to fool users

"You won't find a solution by saying there is no problem."
- William Rostler

History of Phishing

- Phishing is a term for Cons that use technology
  - Example: The Sting (1973 Best Picture)
- A phishing technique using the internet was described in detail as early as 1987
- First recorded use of the term "phishing" was made in 1996 by AOL
- Traditional phishing attacks are sent to millions in hopes of luring some victims

Early Phishing focused on AOL

- A phisher would pose as an AOL staff member and send an instant message to a potential victim, asking him to reveal their password
  - The message might include imperatives like "verify your account" or "confirm billing information”
- Once the victim had revealed the password, the attacker could access and use the victim's account
- Phishing became so prevalent on AOL that they added a line on all instant messages stating: “No one working at AOL will ask for your password or billing information”

From AOL to financial institutions

- The first known direct attempts against a payment system was June 2001 against E-gold.com
- The second attempt was a "post-9/11 ID check" shortly after the September 11 attacks on the World Trade Center
- The first such examples were sent indiscriminately in the expectation that some would be received by customers of a given bank or service
- Purpose is to con a person into giving enough personal information to allow access to a personal account

Early eMail Phishing Example

FROM THE DESK OF THE DIRECTOR.
AUDITING AND ACCOUNTING SECTION,
TEL:+22508534917
E-MAIL: drjcpabou@yahoo.com
BIAO BANK ABIDJAN COTE D'IVOIRE, WEST AFRICA.

I am the director in charge of Auditing and Accounting section of BIAO BANK ABIDJAN COTE D'IVOIRE west Africa. I crave your indulgence as i contact you in such a surprising manner. But I respectfully insist you read this letter carefully as I am optimistic it will open doors for unimaginable financial rewards for both of us.

In my department I discovered an abandoned sum of Ten Million Five Hundred Thousand US dollars (US$10.5m) in account that belongs to one of our foreign customers (Mrs Joyce Lake An america) who died Eight years ago in 2000 a plane crash with the whole passengers aboard Nb;in other for you to believe me honestly go through this (Website) before you start with me Below is the information need
Your bank name, your Name, Your private telephone and fax number, Your Home Address and Occupation

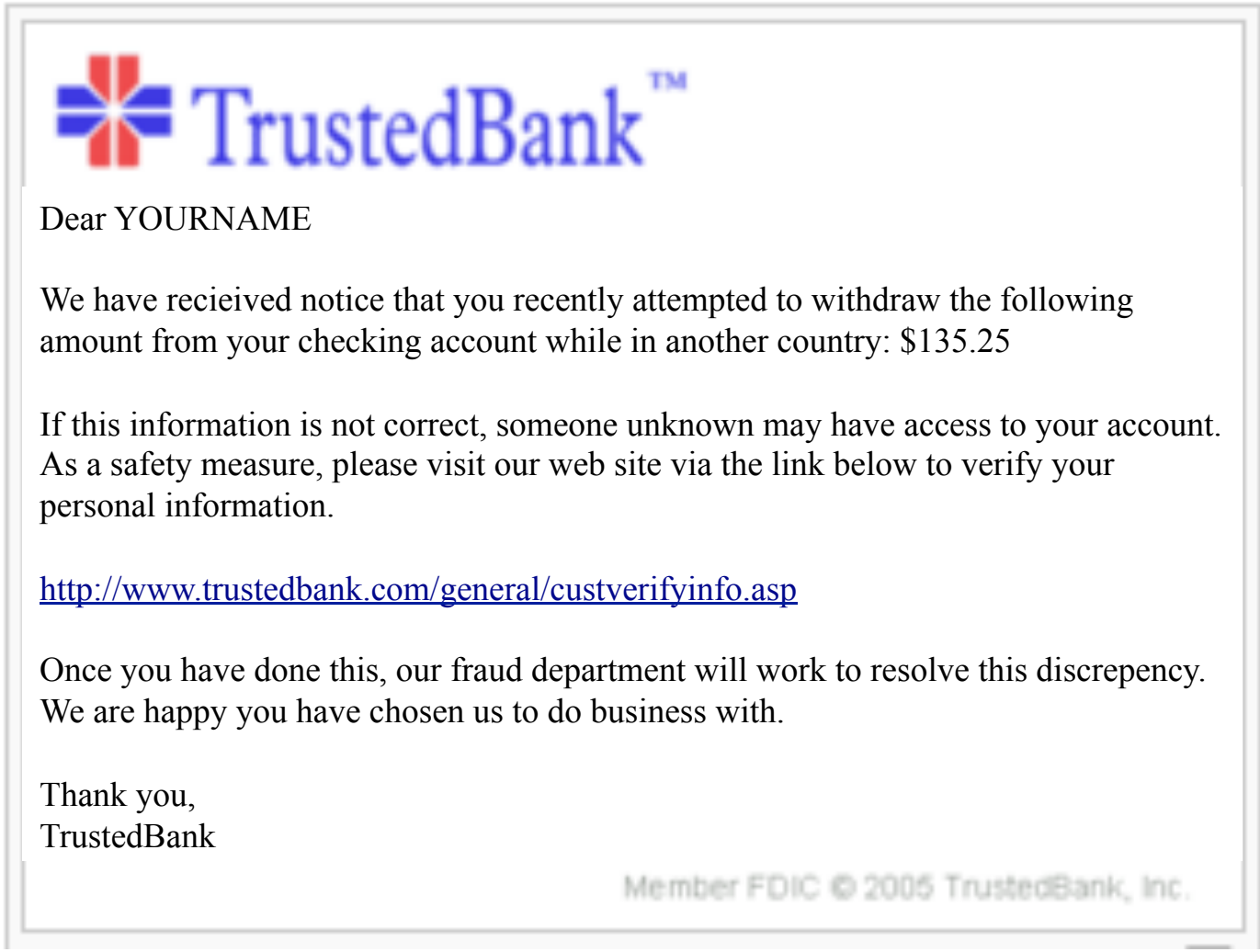
Obvious problems – spelling mistakes, grammar, etc.,
However, Many are almost impossible to differentiate

The Rise of Spear-Phishing

- Phishers now determine which banks potential victims use, and target bogus e-mails accordingly
  - These message contain names of banks and their staff
  - Two groups of criminals have stolen data from an estimated 15,000 victims over the past 15 months, using targeted e-mail attacks, according to researchers at VeriSign
  - This is referred to as Spear-Phishing
- Recent phishing attacks have been directed specifically at senior executives and other high profile targets within businesses.
  - This has been referred to as “whaling”

Spear-Phishing email example

- Disguised as an official e-mail from a bank
- They have your name, email and bank name.
- The sender is attempting to trick the recipient into revealing secure information by "confirming" it at the phisher's website
- The label on the link looks like the TrustedBank URL
- Actual link is the phishers site



TrustedBank™

Dear YOURNAME

We have recieived notice that you recently attempted to withdraw the following amount from your checking account while in another country: $135.25

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our web site via the link below to verify your personal information.

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.

- Note the misspelling of the words received and discrepancy is no longer common
- These spoofs have also come from the IRS and Courts

Phishing Social Network Sites

- Social networking sites are also a target of phishing, since the personal details in such sites can be used in identity theft
- In late 2006 a computer worm took over pages on MySpace and altered links to direct surfers to websites designed to steal login details

Link Manipulation

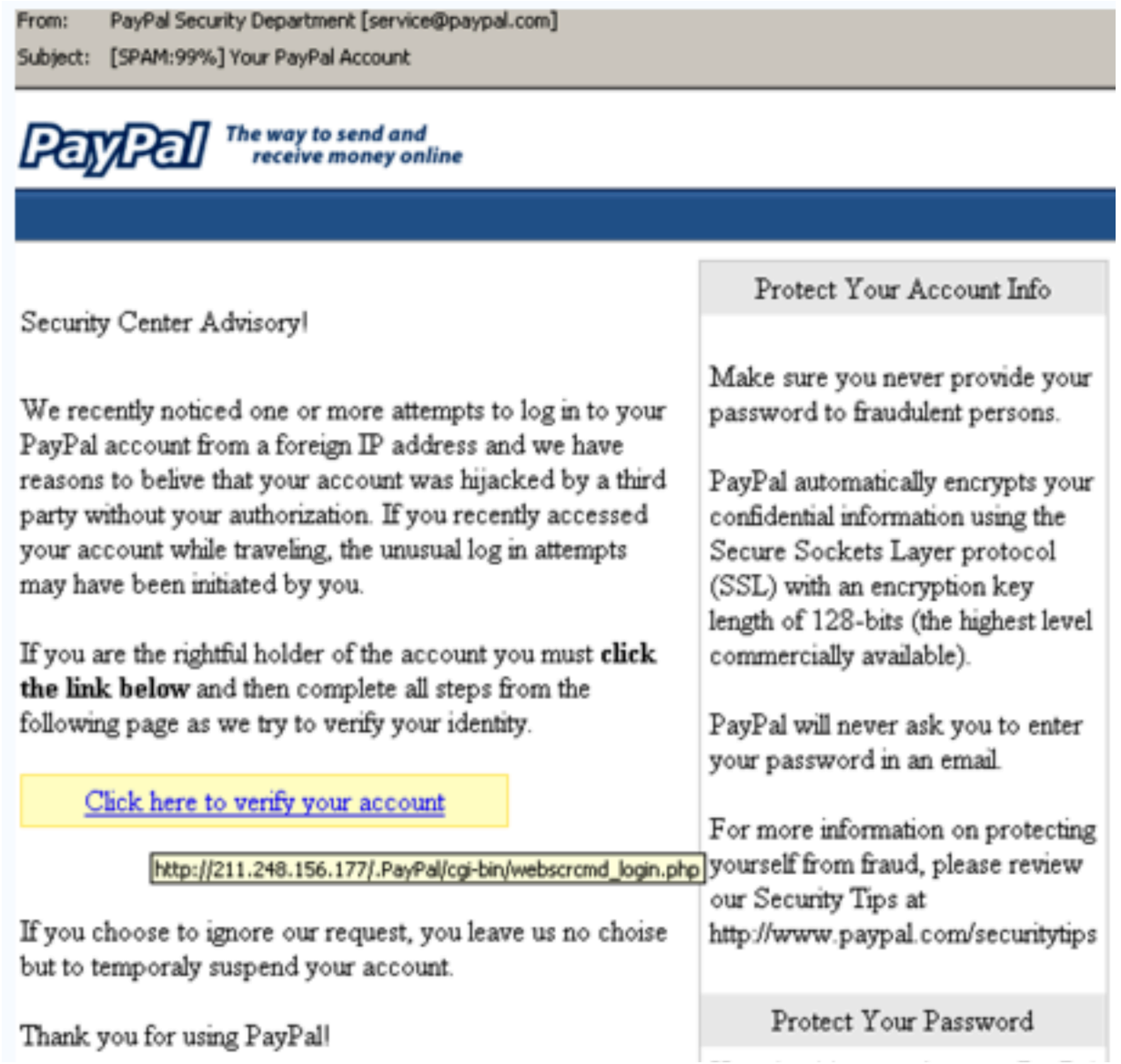
- Deception to make a link in an e-mail appear to belong to the spoofed organization and the spoofed website it leads to
- Misspelled URLs or the use of sub domains:
  - `http://www.yourbank.example.com/`
  - `http://www.yurbanx.com/`
- Another common trick is to make the anchor text for a link appear to be valid, when the link actually goes to the phishers' site. For Example:
  - the label on the link looks like the URL http://www.yourbank.com
  - but the actual link is <href=”http://www.badguy.net">

NEVER click on a link, even if it looks real

eBay Link Manipulation Example

Clues:

- Spelling mistakes in the e-mail (Not as common as before)
- Disgused Links
  - An IP address in the link (When Cursor is over link)
- Threat of consequences



From: PayPal Security Department [service@paypal.com]
Subject: [SPAM:99%] Your PayPal Account

PayPal The way to send and receive money online

Security Center Advisory!

We recently noticed one or more attempts to log in to your PayPal account from a foreign IP address and we have reasons to belive that your account was hijacked by a third party without your authorization. If you recently accessed your account while traveling, the unusual log in attempts may have been initiated by you.

If you are the rightful holder of the account you must **click the link below** and then complete all steps from the following page as we try to verify your identity.

Click here to verify your account

http://211.248.156.177/.PayPal/cgi-bin/webscrcmd_login.php

If you choose to ignore our request, you leave us no choise but to temporaly suspend your account.

Thank you for using PayPal!

Protect Your Account Info

Make sure you never provide your password to fraudulent persons.

PayPal automatically encrypts your confidential information using the Secure Sockets Layer protocol (SSL) with an encryption key length of 128-bits (the highest level commercially available).

PayPal will never ask you to enter your password in an email.

For more information on protecting yourself from fraud, please review our Security Tips at http://www.paypal.com/securitytips

Protect Your Password

Vishing: Phone Phishing

- Messages that claimed to be from your bank told users to dial a phone number regarding problems with their bank accounts
- Once the phone number (owned by the phisher, and provided by a Voice over IP service) was dialed, prompts told users to enter their account numbers and PIN
- Vishing (voice phishing) sometimes uses fake caller-ID data to give the appearance that calls come from a trusted organization

Social Engineering Phishing

- Social engineering techniques are based on specific attributes of human decision-making known as cognitive biases
- These biases are exploited in various combinations to create attack techniques, some of which are listed here:
  - Pretexting is the act of creating and using an invented scenario to persuade a target to release information or perform an action
  - Use of known information (date of birth, Social Security Number, last bill amount) to establish legitimacy in the mind of the target

Snail Mail Phishing

- Companies have received official looking letters requesting fees
- Example:
  - A letter from the "Compliance Annual Minutes Board" asking for an "annual fee" of $150
  - It is not from the State of California and it is not required to be filed
  - The letter is official looking and is confusingly similar to the layout of the Statement of Information that must be filed each year

Actual form on next slide

Official Looking Seal

COMPLIANCE ANNUAL MINUTES BOARD

DIRECTORS AND SHAREHOLDERS

INSTRUCTION FORM

(DOMESTIC STOCK CORPORATIONS) **Annual Fee $150**

CORPORATION NUMBER #: 3079710	NOTICE DATE: 6 / 9 / 08	REPLY BY: June 19, 2008

NAME OF CORPORATION: (Please correct any changes that apply)

CONVERGENT INFORMATICS, INC.
301 SCIENCE DR STE 110
MOORPARK, CA 93021-2095

Correct Information
Form is similar to other Gov't forms

Maintaining records is vital to the existence of all corporations; in particular the recording of shareholder and director meetings. Failure to comply with certain requirements could cause your corporation to lose its limited liability status (Pierced Veil). If so, personal liability or exposure to tax agencies, or creditors, could possibly be put on directors and shareholders for failing to document formalities. Complete the instruction form by providing the following candidate names for the position listed an
delay of our preparation and fulfillment of Annual Minutes for your corporation
provides corporations with minutes in order to keep compliance with applicable la
AND PAYMENT OF $150 TO: COMPLIANCE ANNUAL MINUTES BOARD
12012 HEMET, CA 92546 For Questions? Please, Call: (866) 390-1176

COMPLETE THE ADDRESSES FOR THE
PLEASE, PRINT LEGIBLE IN BLUE OR BL

STREET ADDRESS OF PRINCIPAL EXECUTIVE OFFICE

PRINCIPAL LOCATION OF BOOKS, RECORDS, AND MINUTES:

OFFICER SECTION 1> Enter the name and complete business address of an
Secretary and Treasurer). The corporation must have these three officers (Corp

DIRECTOR SECTION 2> Enter the name and complete business or residentia
are more than three directors please attach additional pages. The corporation
section 301(a).)

SHAREHOLDER SECTION 3> Enter the name and complete business or resi
there are more than three shareholders please attach additional pages.

SEC.1 >PRESIDENT:
SECRETARY:
TREASURER:
SEC.2 > DIRECTOR # 1
DIRECTOR # 2
DIRECTOR # 3
SEC.3 > SHAREHOLDER · (If applicable)
SHAREHOLDER· (If applicable)

2nd page contains many warnings…

Always a clue.

BUSINESS DIVISION NOTIFICATION

CALIFORNIA CORPORATIONS CODE STATES:

SEC. 9510 (A) Each corporation shall keep: (1) Adequate and correct books and records of account. (2) Minutes of the proceedings of its members, board and committees of the board. (3) A record of its members giving their names and addresses and the class of membership held by each. (b) Minutes shall be kept in written form.
SEC. 600 This shall not limit the requirement for holding annual meetings.

Proper Corporate Minutes can save your business from possible dissolution and/or bankruptcy. Once your business has been discredited, it can lose its legal protections, deductions and its very status as a corporation.

Minutes are required regardless of size of company or its board of directors. Both S and C corporations must keep corporate minutes appropriately for compliance with applicable laws and regulations.

SEC.1500 Each corporation shall keep adequate and correct books and records of account and shall keep minutes of the proceeding of its shareholders, board and committees of the board and shall keep at its principal executive office, or at the office of its transfer agent or registrar, a record of its shareholders, giving the name and addresses of all shareholders and the number and class of shares held by each. Such minutes shall be kept in written form. Such other books and records shall be kept either in written form or in any other form capable of being converted into written form.

FEE: $150 should be submitted for processing and fulfillment of the Annual Minutes for your corporation. Submit a single check or money order made payable to Compliance Annual Minutes Board and mail to:

COMPLIANCE ANNUAL MINUTES BOARD
BUSINESS DIVISION P.O. BOX 12012
HEMET, CA 92546

By submitting the Disclosure Form of Directors and Shareholders to Compliance Annual Minutes Board Business Division. The corporation certifies the information contained herein, including any attachments is true and correct.

DOC 21 CAMB(REV. 8/2006)

California Corporations Code Sec 1500, 600, 9510: Is Statutory And Your Corporation Should Comply With Applicable Laws And Regulations For Adequate Record Transfer, **Please Print Legible.** All Information Will Be Treated As Private And Confidential. Please Allow 30 Days From The Date of Receipt For Complete Processing, Fulfillment, And Mailing of The Annual Minutes For Your Corporation. **California B & P Code: 17533.6** This Product or Service Has Not Been Approved or Endorsed By Any Government Agency And This Offer Is Not Being Made By An Agency of The Government. **Attorneys And Accountants Typically Charge $200 To 700** For Annual Minutes Preparation. **CAMB** Prepares Annual Minutes That Meet California Statutory [illegible] Solicitation For The Order Of Services, And Not A Bill, Invoice Or Statement Of Account Due. No Obligation To Make Any Payments; Unless You Accept This Offer.

By submitting the above corporate information to Compliance Annual Minutes Board, the corporation certifies the information herein, including any attachments, is true and correct.

SIGNATURE OF OFFICER: TITLE: DATE:

No Obligation To Make Any Payments; Unless You Accept This Offer.

COMPLIANCE ANNUAL MINUTES BOARD
BUSINESS PROCESSING DIVISION
P.O. BOX 12012
HEMET, CA 92546

Return Address Label
Not a Government Document

BUSINESS MAIL – IMPORTANT NOTICE ENCLOSED
THIS IS NOT A GOVERNMENT DOCUMENT

Know the Laws

- No court subpoenas or served papers via email
- No financial institution will ask for your pin or password
- Be Aware
  - Be sensitive to anyone asking for any personal information
  - Before you provide any information, ask yourself "why do they need this information"
  - Be especially careful, if they call/contact you – how do you know the person is who they say they are? –
    - If you're not sure, call them back

Information Security

- These cons are
  - Coming faster
  - Getting harder to detect
- Make sure that you are always 100% sure who you are communicating with

"Be afraid. Be very afraid."
- The Fly (985) Geena Davis (as Veronica Quaife).

Glossary

- Phishing
  - To criminally and fraudulently acquire sensitive information, such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication.
- Vishing:
  - The criminal practice of using social engineering and Voice over IP (VoIP) to gain access to private personal and financial information from the public for the purpose of financial reward.
- Spim:
  - A type of spam targeting users of instant messaging (IM) services.